BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

Tesztlaborok gombnyomásra

Höltzl Péter, senior trainer

HOUG konferencia, Április 2018

Miről lesz szó?

- Mitől lesz jó egy training?
- Milyen kihívások vannak egy labor környezet felépítésében
- Hogyan építettük fel a Balabit labor környezetét?

A Balabit bemutatása

- 18 éve az IT Security-ben
- 1300+ ügyfél
- 100+ Partner
- 25+ Fortune 100-as ügyfél
- Irodák: Budapest, New York, London, Párizs, München, Moszkva
- 2018-tól a Quest/One Identity része

Termékeink

- Termékek:
  - Zorp (2015-ig)
  - PSM (ex SCB) (2006 óta)
  - syslog-ng OSE és PE (1999 óta)
  - syslog-ng Store Box (2009 óta)

Technical trainingek

- Instructor-led, classroom based
- On-site training
- Termékek szerint:
  - PSM Technical Training
  - syslog-ng Technical Training
  - syslog-ng Store Box Technical Training
  - Troubleshooting Technical Training

Milyen egy jó training?

- Elmélet, Gyakorlat (Labor) megfelelő arányban
- Prezentáció
- Feladatok és Exercise Book (sokszor nyomtatva)
- Mindenkinek teljesen ugyanaz a környezet

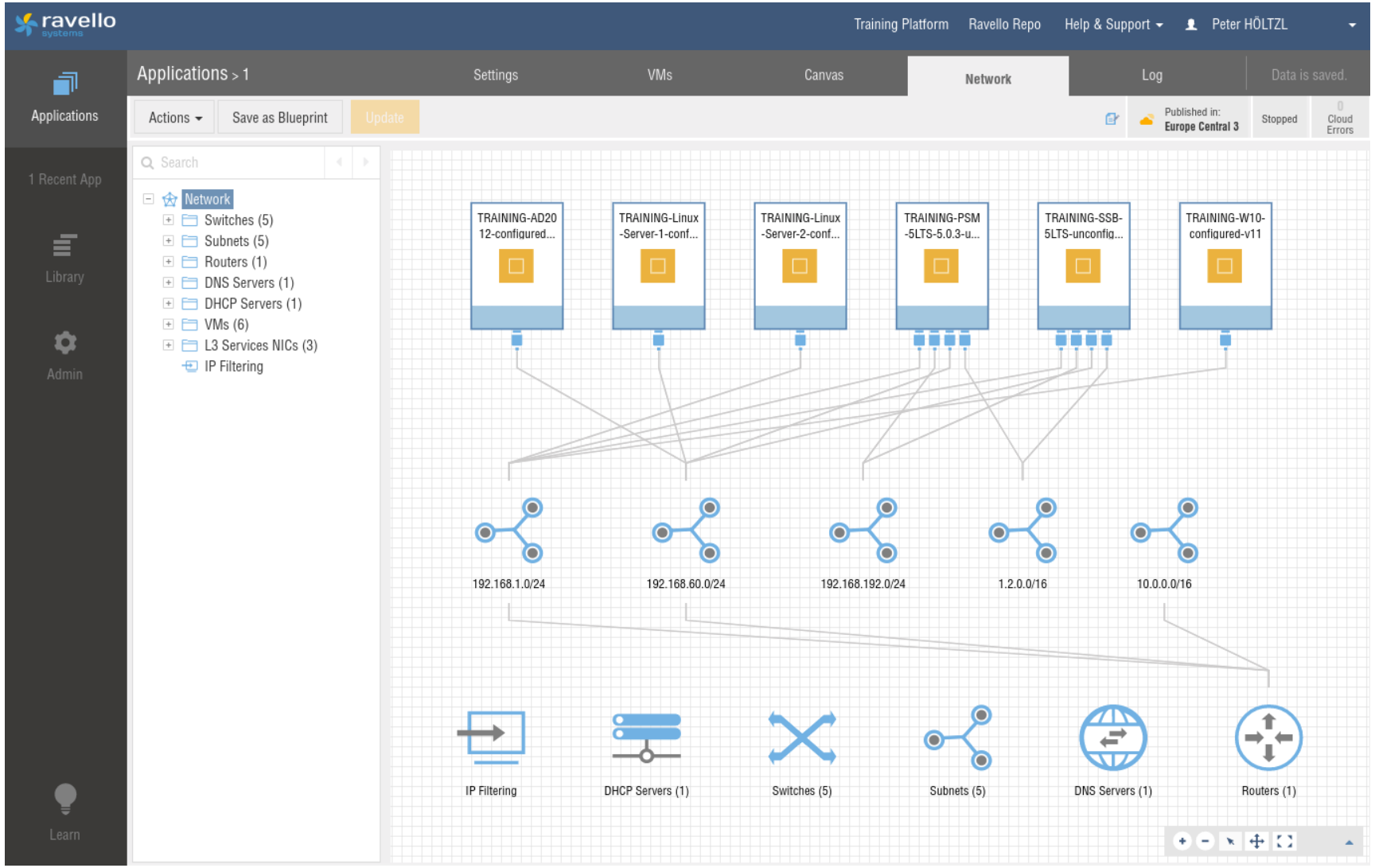
Milyen problémákba ütköztünk

- Saját hosting
  - Erőforrás igény
  - Üzemeltetés, karbantartási igény, frissítések
  - Elérés, latency
- Hallgatói hosting
  - Mindenkinek más a rendszere
  - A saját gépemen nincs virtualizáció engedélyezve
  - A gépem lassú, kevés az erőforrás (következő slide)
  - Nem tudom a BIOS jelszót!

Erőforrás igény

- PSM: 5 host, 6 core, 24GB RAM, 100Gb Storage, 2 network (~1.2USD/h)
- syslog-ng/SSB: 4 host, 5 core, 16GB RAM, 60GB storage, 1 network (~0.8USD/h)
- Troubleshooting: 6 host, 7 core, 28GB RAM, 100Gb Storage, 2 network (~1.4USD/h)

Topológia



BALABIT

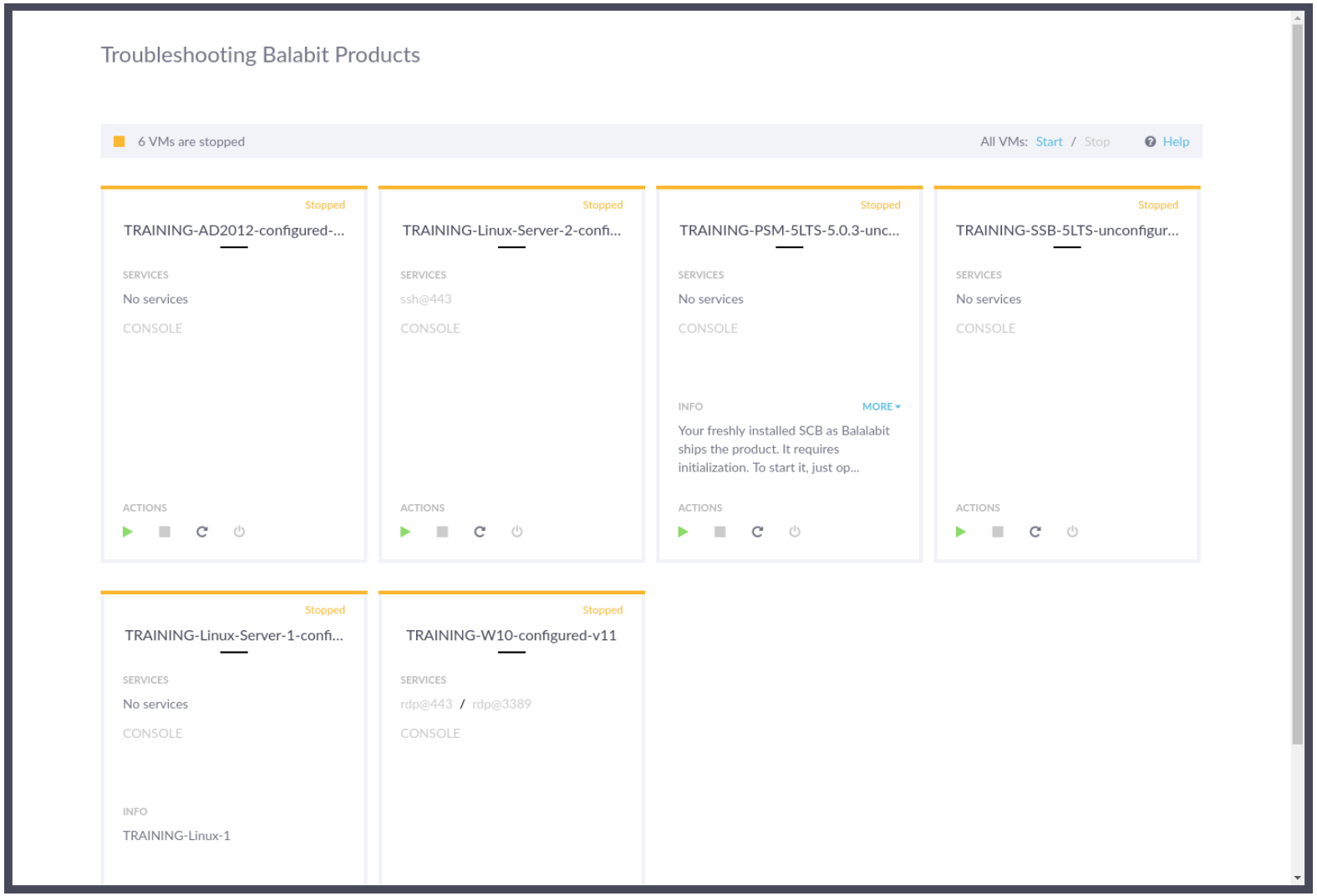
Kellett egy megoldás, ami(t)...

- Nem mi üzemeltetünk
- Template alapú (blueprint)
- Mindenhol elérhető
- Könnyen elérhető (RDP)
- Minden hallgatónál egyforma
- A hallgatókat elkülöníti
- Automatizált
- Illeszthető a rendszerünkhöz (van API)
- Megy a mi termékünk (nem XEN álló): HVX

Itt jött a képbe a Ravello

- Importált image-ek (VM)
  - Ravello import tool (linux is!)
- Blueprint: template környezet
- App: A blueprint materializálása
- Ephemeral Access: Időzített access a Ravello account nélküli felhasználóknak
- Elastic IP
- Port forward (külső hozzáférés)

Mit lát a hallgató?



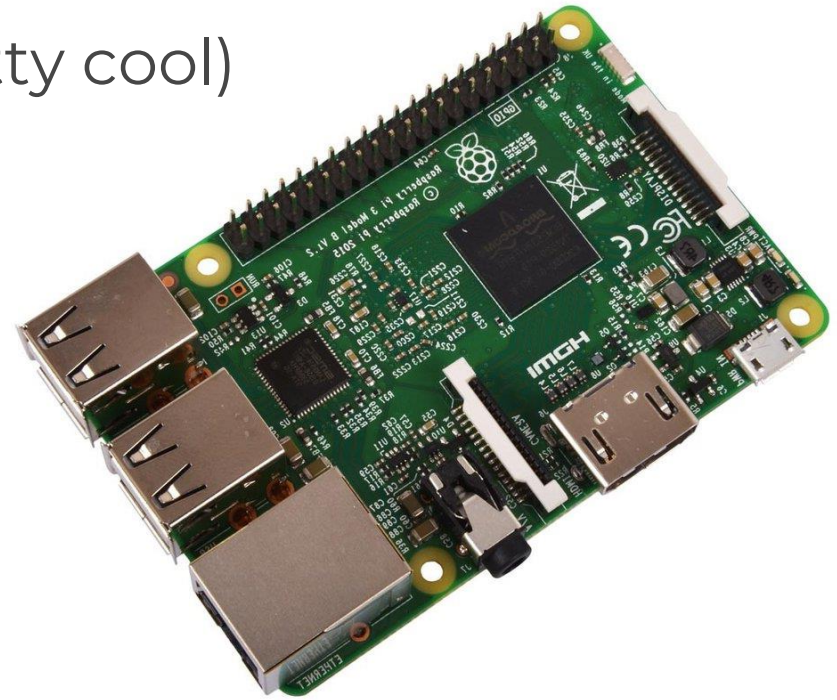
BALABIT

Integráció

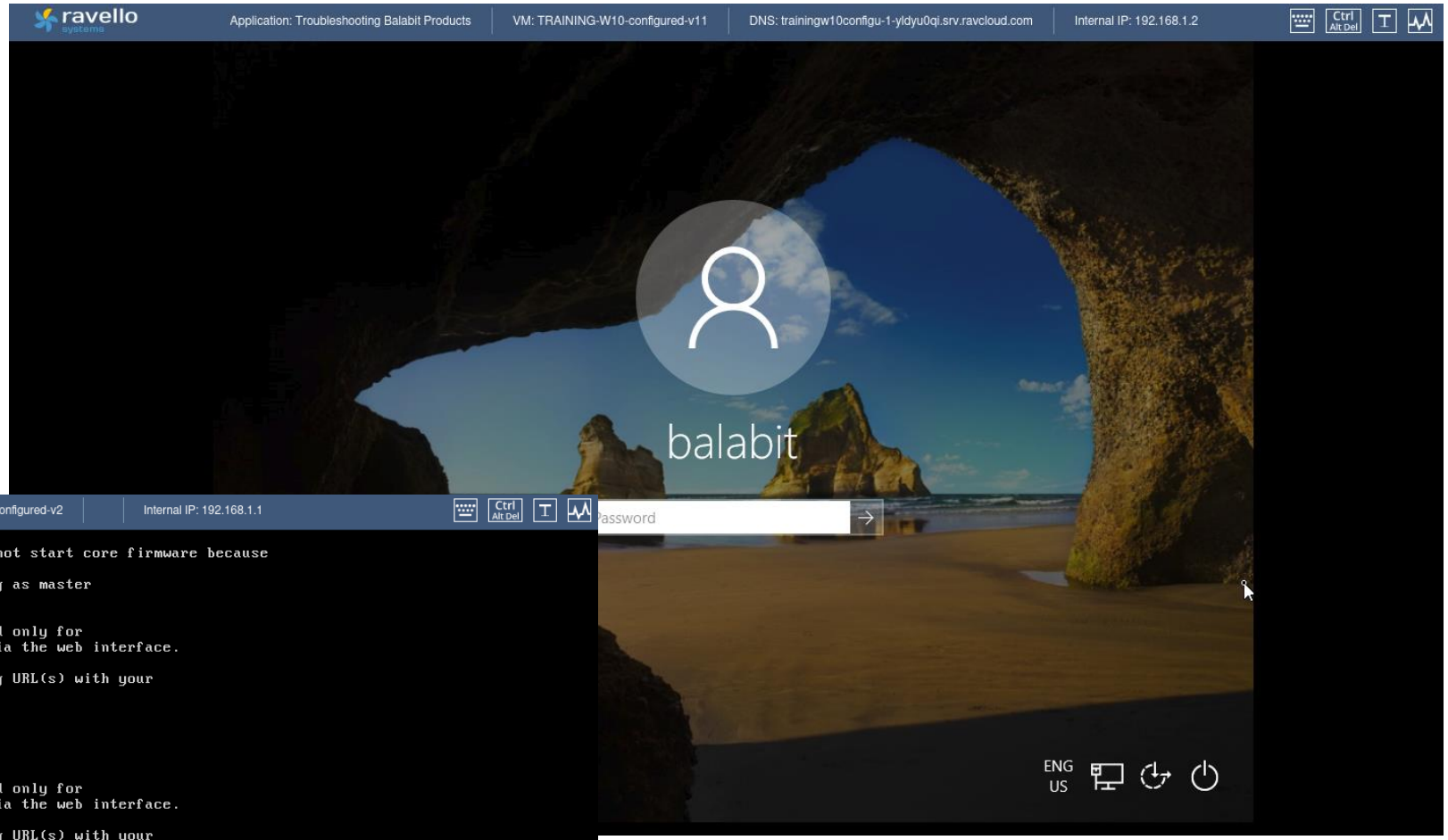
- Ravello API + MyBalabit integráció
- App legyártása Blueprint ID-ból
- Ephemeral Access legyártása → Link a mybalabit-en
- Training után Ephemeral törlése
- Training után App törlése

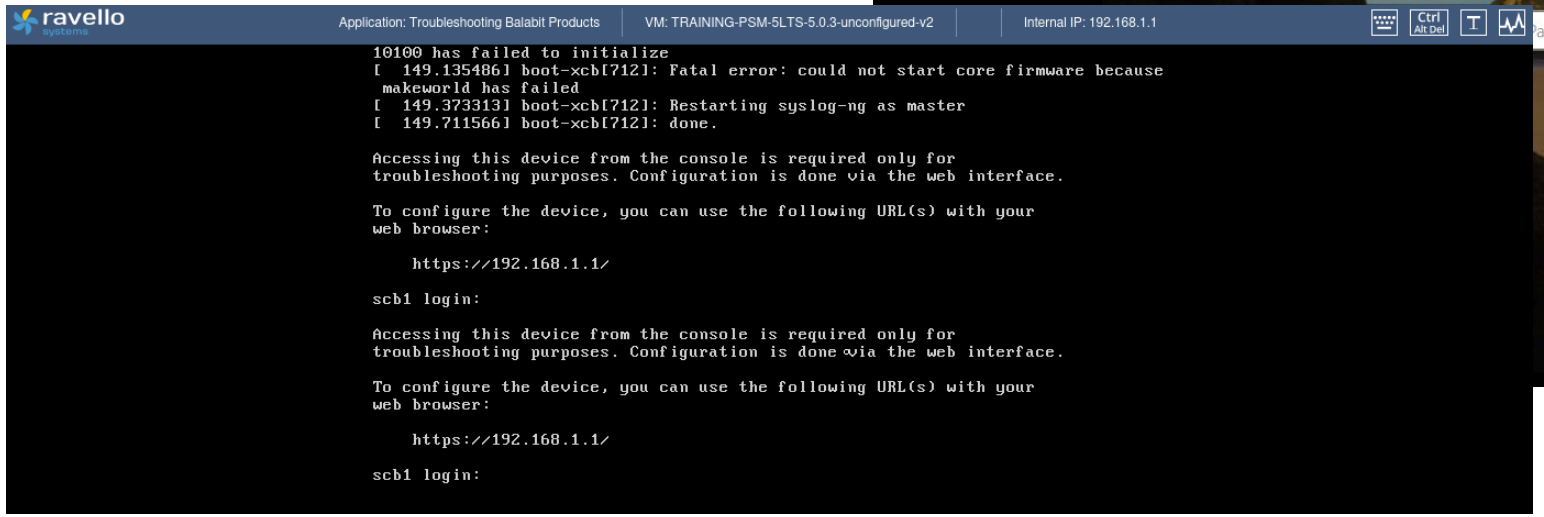
Hozzáférés

- Console (VNC over HTTPS)
- PortForward (Windows 10 Jumphost + RDP)
- Balabit training room:
  - Raspberry Pi + Ubuntu MATE (olcsó és pretty cool)



Mit lát a felhasználó?





Nice features

- Share blueprint (bárkivel, akinek van oracle access-e)
- Cost alert
- Buckets
- Scheduling

Ami jól jönne

- Okosabb port forward (PAT)
- 3D támogatás (OpenGL)
- App relokáció
- Training platform API támogatás

Q&A

Höltzl Péter
peter.holtzl@balabit.com